

## In the Iowa Supreme Court

In the Matter of the )  
 Independent Investigation Into )  
 Judicial Branch Information )  
 Security Testing )

## Supervisory Order

CLERK SUPREME COURT

On September 20, 2019, the Iowa Supreme Court engaged outside counsel to conduct an independent investigation into the September 11, 2019, arrest in the Dallas County Courthouse of two individuals and the September 9, 2019, alleged break-in at the Polk County Courthouse. Both events appear to have occurred during information security testing exercises intended to help the Iowa Judicial Branch ensure the court's highly sensitive data was secured against attack.

Outside counsel has submitted its report to the supreme court and the report can be found on the judicial branch website. The supreme court has reviewed the independent investigative report and directs state court administration to follow these policies in the future effective immediately:

- All information security contracts must undergo legal review.
- The state court administrator must personally approve contracts involving sensitive security information and penetration testing.
- State court administration must also include input from building security, sheriffs, and other physical security professionals in any Red Team<sup>1</sup> planning.
- All penetration testing<sup>2</sup> or Red Team contracts must have precise

---

<sup>1</sup>"Red Teams ('ninjas') have one primary objective—'get in.' Sometimes considered a subset of pen testing, Red Teams typically take more time, provide little or no notice to the defending team, and try to enter computer networks using a combination of stealthy online or real-world *physical* techniques." Coalfire Investigation Report, p.2.

<sup>2</sup>"Pen testers ('pirates') are also called 'white hat' or 'ethical hackers' and they often try to test as many different network vulnerabilities as possible by surveilling, probing, and attacking client systems using *online* techniques. Pen testers often work within a prescribed time period, with or without notice to the defending IT security team." *Id.*

terminology. There must be clear statements of what is permitted and what is prohibited and the contracts must distinguish between “physical testing” and “penetration testing.”

- Contracts must prohibit entry into courthouses for any reason outside of normal business hours and must prohibit physical break-ins regardless of time.
- Before engaging in any security assessment, state court administration must confer with local law enforcement and other state and local officials that could be affected by the assessment.

Dated this 10th day of October, 2019.

The Iowa Supreme Court

By



Mark S. Cady, Chief Justice